Le routeur Turris Omnia

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 octobre 2016

https://www.bortzmeyer.org/turris.html

Je viens d'installer chez moi un routeur Turris Omnia <https://www.turris.cz/en/>. Ça fait quoi et ça sert à quoi ?

Voici ce routeur avec ses copains et copines (sonde RIPE Atlas <https://atlas.ripe.net/> et Raspberry Pi de supervision <https://www.bortzmeyer.org/icinga.html>) : (Version non réduite (en ligne sur https://www.bortzmeyer.org/files/turris-on-LARGE.jpg)) Rassurez-vous, on peut contrôler par un bouton la luminosité des diodes (très intense par défaut).

Le Turris Omnia <https://omnia.turris.cz/en/> est avant tout un routeur pour la maison ou la petite entreprise. En tant que routeur, il... route, c'est-à-dire qu'il fait passer les paquets d'un réseau à l'autre, en l'occurrence entre le réseau de la maison et celui du FAI et, via ce dernier, à tout l'Internet. C'est donc l'équivalent de la "*box*" qui, en France (mais pas ailleurs) est souvent fournie par le FAI.

La différence principale est que l'Omnia ne comprend que du logiciel libre et est ouvert, au sens où on est super-utilisateur sur cette machine et où on peut la configurer comme on veut, contrairement aux "*boxes*" fermées dont on ne sait pas exactement ce qu'elles font (elles peuvent par exemple surveiller le trafic, même local <https://lauren.vortex.com/2016/07/24/how-some-isps-could-subvert-your-local L'Omnia n'est pas conçu par une boîte commerciale mais par le registre du .cz, une organisation sans but lucratif (qui développe des tas de choses intéressantes).

D'autre part, des tas de services qui devraient être de base en 2016 (IPv6, validation DNSSEC) sont disponibles en série sur l'Omnia.

Si vous n'êtes pas technicien, je vous préviens que l'Omnia est installable et configurable sans trop de difficultés mais que toute adaptation un peu sérieuse nécessite, pour l'instant, de bonnes compétences d'administrateur système et réseau.

Suivons maintenant l'ordre chronologique de la mise en route. Commençons par le matériel. Voici l'Omnia vue de devant, posée sur le T-shirt (optionnel...) : (Version non réduite (en ligne sur https://www.bortzmeyer.org/files/turris-outside-front-LARGE.jpg)).

Je n'ai pas encore essayé la console série, il faudrait ouvrir la boîte et connecter les fils <https://docs.turris.cz/hw/serial/>. Voici l'arrière de la boîte. Les antennes Wi-Fi ne sont pas encore montées (les connecteurs dorés en haut). Le port SFP est rare sur ce genre de routeurs à la maison, mais je ne l'ai pas encore utilisé (il peut permettre des connexions directes à une fibre optique, par exemple) : (Version non réduite (en ligne sur https://www.bortzmeyer.org/files/turris-outside-back-LARGE.jpg)).

Et voici l'Omnia ouverte, pour les amateurs d'électronique (la documentation du matériel est en ligne <https://www.turris.cz/doc/en/howto/omnia_manuals>) : (Version non réduite (en ligne sur https://www.bortzmeyer.org/files/turris-inside-LARGE.jpg)). Curieusement, une vis avait été oubliée à l'intérieur... J'ai découvert par la suite que c'était une des vis censées tenir les cartes Wifi. Le Turris Omnia a <https://omnia.turris.cz/en/#features> 1 ou 2 Go de RAM (j'ai le modèle à 1 Go), un processeur ARM à 1,6 Ghz, une Flash de 8 Go, et quelques trucs que les électroniciens adoreront comme des ports GPIO.

Attention à vérifier les connecteurs des antennes radio. Dans mon cas, ils étaient mal vissés, ce qui faisait que les antennes tombaient et, ce faisant, tournaient la petite carte située derrière les connecteurs, ce qui arrachait le fil menant à la carte WiFi. Bien serrer ces connecteurs avant de commencer.

Branchons-la, maintenant. Je suis abonné chez Free et, par défaut, c'est leur boitier qui fait l'interface physique avec la ligne ADSL (de toute façon, l'Omnia n'a pas de prise adaptée <https://www.turris.cz/en/hardware#hw-smrt>, à moins de passer par le SFP ?). J'ai donc décidé de garder la Freebox, mais elle s'occupe uniquement de la télévision, du téléphone fixe, et du branchement à l'ADSL. Tout le routage, le réseau local et le Wi-Fi sont faits par l'Omnia. Je laisse donc le "*Freebox Player*" (la boîte qui sert à la télé) branchée au "*Freebox Server*" (la Freebox proprement dit), comme avant. Et je passe la Freebox en mode « bridge » <http://www.free.fr/assistance/5082.html>. Avec cette configuration, la télévision classique continue à fonctionner (regarder la télévision, gérer ses enregistrements via http://mafreebox.freebox.fr/, etc). Le téléphone marche aussi. Pour le reste, je branche la prise WAN de la Turris Omnia en Ethernet, sur le commutateur du "*Freebox Server*". Les autres machines sont branchées sur le commutateur de l'Omnia (ou utilisent son Wi-Fi). Il y a cinq ports Ethernet utilisables.

Une fois l'Omnia et au moins un PC branché, on configure le routeur via le Web, en se connectant à http://192.168.1.1/ (rassurez-vous, tout cela est bien expliqué dans le joli manuel papier de quatre pages livré avec l'Omnia, ou bien en ligne <https://www.turris.cz/doc/_media/en/howto/omnia_manual_en.pdf>. Il y a **deux** interfaces Web de configuration du Turris Omnia, Foris <https://www.turris.cz/doc/en/howto/foris>, orientée débutant, et spécifique à l'Omnia, et LuCI <https://github.com/openwrt/luci/wiki>, bien plus riche, dont je parlerai plus longuement après. Voici ce que voit le célèbre M. Michu, lorsqu'il utilise Foris : Free ne fournit apparemment pas de mécanisme pour la configuration automatique d'IPv6, il a donc fallu la faire à la main, statiquement.

Contrairement au Turris précédent, cette fois, on n'est plus obligé de parler la langue de Karel [Caractère Unicode non montré [1]]apek avec l'Omnia. Presque tout est traduit. (Mais pas encore les divers HOWTO en ligne <https://www.turris.cz/doc/en/howto/start>.) C'est un progrès appréciable pour le non-polyglotte qui, en 2014, avec l'ancien Turris, recevait des notifications du genre « *"Upozorneni od Vaseho routeru Turris ##### Oznameni o aktualizacich ##### [Caractère Unicode non montré] Nainstalovan[Caractère Unicode non montré] verze 82 bal[Caractère Unicode non montré]ku updater..."* ». La documentation de Foris <https://www.turris.cz/doc/en/howto/foris> est très détaillée,

1. Car trop difficile à faire afficher par LaTeX

et il est recommandé de la lire (par exemple pour configurer le Wi-Fi, lorsque Foris demande à M. Michu s'il veut du 2,4 GHz ou du 5 GHz... Au passage, l'Omnia peut faire les deux, en configurant deux interfaces avec des fréquences différentes, ce qui ne semble possible qu'avec LuCI ou le fichier texte de configuration.)

Si on découvre des bogues à signaler, il faut écrire à `info@turris.cz` qui répond bien. Il y a aussi un canal IRC `#turris` à Freenode (peu d'activité). Questions forums collectifs, il y avait un système de forums (avec les menus uniquement en tchèque) qui a été abandonné au profit de Discourse <https://discourse.labs.nic.cz/c/turris-omnia>, que je recommande d'utiliser (on a des réponses). Il est apparemment nécessaire, pour se loguer, d'avoir mojeID <https://www.bortzmeyer.org/moje-id.html> (ce que j'utilise) ou bien un compte sur un GAFA.

Ensuite, tout fonctionne, le routeur route, on peut regarder des vidéos de chats, envoyer du courrier, parler avec les copains en XMPP, télécharger de la culture, etc.

Notez que le routeur est sécurisé par défaut. Le pare-feu interne, dans sa configuration d'origine, bloque les connexions entrantes. (IPv4 et IPv6, bien sûr, une fonction qui manque terriblement à la Freebox, cf. RFC 6092 [2].) De même, le routeur a SSH et un résolveur DNS mais n'accepte pas les connexions SSH ou DNS de l'extérieur. (Parfois, c'est même trop sécurisé <https://discourse.labs.nic.cz/t/cannot-ping-the-router-from-outside-over-ipv4/>.)

Une autre particularité du Turris Omnia est que le routeur se met à jour tout seul, récupérant automatiquement les nouvelles versions des logiciels, afin de corriger notamment les failles de sécurité (c'est évidemment configurable, via l'onglet "*Updater*" de Foris). C'est en effet une défaillance courante chez ces petits engins installés à la maison : le code n'est pas mis à jour et de vieilles failles durent longtemps. Tous les matins, on peut voir sur Foris ce qui a été changé :

On peut aussi le recevoir via le système de notification par courrier. Le Turris peut envoyer des messages via les MTA de NIC.CZ ou bien via le vôtre si vous la configurez ainsi (dans "*Maintenance*").

Le Turris permet également d'envoyer ses données de trafic dans le nuage. Ce n'est évidemment pas activé par défaut mais, si on veut aider la science, cela se fait par l'onglet "*Data collection*" de Foris (« "*we'd like to inform you that you agreed with our EULA regarding data collection of your router*" »). Une fois cet envoi activé, et un compte sur le portail créé via le Turris, on pourra se connecter sur le portail <https://www.turris.cz/en/user/login> (mojeID <https://www.bortzmeyer.org/moje-id.html> était nécessaire mais ce n'est plus le cas) et voir des jolis graphes de son trafic :

Naturellement, l'administrateur système consciencieux, même s'il se nomme Michu, va faire des sauvegardes. L'interface Foris a une option "*Configuration backup*" dans son onglet "*Maintenance*".

Passons maintenant à l'interface Web avancée, LuCI <https://github.com/openwrt/luci/wiki>. Elle n'est pas spécifique à l'Omnia et est au contraire bien connue des utilisateurs d'OpenWrt, système sur lequel est bâti l'Omnia. Ce n'est pas génial d'avoir deux interfaces Web pour la configuration, je trouve. Mais LuCI est indispensable pour les fonctions avancées, comme la configuration du pare-feu. Voici l'écran principal de LuCI :

2. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6092.txt`

LuCI peut servir à regarder l'état de certaines fonctions, ici le pare-feu :

Mais aussi à configurer des fonctions comme, ici, le commutateur interne avec ses VLAN (je n'ai pas encore testé mais cela semble nécessaire si on veut connecter le Freebox Player au réseau local <https://guillaume.vaillant.me/?p=256>):

On peut aussi installer des programmes supplémentaires depuis LuCI. Le premier que j'ai mis était Majordomo <https://www.turris.cz/doc/en/howto/majordomo> (rien à voir avec le gestionnaire de listes de diffusion du même nom). Il permet d'intéressantes statistiques par machine (là aussi, quelque chose qui me manque sur la Freebox) :

Le vrai "*geek*" va sans doute vouloir se connecter à son beau routeur libre en SSH (chose qu'on ne peut certainement pas faire avec la Freebox...). Une fois le serveur activé ("*Advanced administration*" dans Foris mais attention avec SSH, une bogue sérieuse est décrite plus loin) :

```
% ssh root@turris
Password:

BusyBox v1.23.2 (2016-09-05 13:26:40 CEST) built-in shell (ash)

  _______  _    _  _____   _____   _____   _____
 |__   __|| |  | ||  __ \ |  __ \ |_   _| / ____|
    | |   | |  | || |__) || |__) |  | |  | (___
    | |   | |  | ||  _  / |  _  /   | |   \___ \
    | |   | |__| || | \ \ | | \ \  _| |_  ____) |
    |_|    \____/ |_|  \_\|_|  \_\|_____||_____/


root@turris:~# sensors
armada_thermal-virtual-0
Adapter: Virtual device
temp1:        +86.1°C
```

Notez que je ne connais pas de moyen de connaitre le condensat de la clé publique SSH créée, depuis l'interface Web. On ne peut donc pas vérifier, la première fois, qu'on se connecte bien à son Turris Omnia.

Le Turris Omnia utilise <https://www.turris.cz/en/software> OpenWrt, un Unix (avec noyau Linux). La plupart des commandes seront donc familières aux unixiens :

```
root@turris:~# uptime
 11:32:39 up 1 day,  3:35,  load average: 0.02, 0.05, 0.01

root@turris:~# df -h
Filesystem                Size      Used Available Use% Mounted on
/dev/mmcblk0p1            7.3G    180.5M      7.1G   2% /
tmpfs                   503.7M      6.9M    496.9M   1% /tmp
tmpfs                   512.0K      4.0K    508.0K   1% /dev

root@turris:~# dig fr.wikipedia.org

; <<>> DiG 9.9.8-P4 <<>> fr.wikipedia.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38235
```

```
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fr.wikipedia.org. IN A

;; ANSWER SECTION:
fr.wikipedia.org. 3 IN A 91.198.174.192

;; Query time: 7 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Oct 19 11:36:54 UTC 2016
;; MSG SIZE  rcvd: 61

root@turris:~# uname -a
Linux turris 4.4.13-05df79f63527051ea0071350f86faf76-7 #1 SMP Mon Sep 5 13:01:10 CEST 2016 armv7l GNU/Linux
```

Pour mémoire, l'ancien Turris, avant l'Omnia, affichait :

```
root@turris:~# uname -a
Linux turris 3.10.18-b09ae823eeafb345725b393bc5efbba7 #1 SMP Tue May 6 16:24:28 CEST 2014 ppc GNU/Linux
```

Et n'avait que 250 Mo de stockage.

Le résolveur par défaut du Turris Omnia, l'excellent Knot Resolver <https://www.knot-resolver.cz/> (produit par la même organisation que Turris), valide avec DNSSEC (comme tout le monde devrait faire, en 2016). Dommage, il reste encore des sérieuses bogues (comme une mauvaise indication du résultat <https://gitlab.labs.nic.cz/knot/resolver/issues/98> ou comme l'impossibilité de couper la validation <https://gitlab.labs.nic.cz/knot/resolver/issues/97>).

Un des avantages du shell est qu'on peut faire tout ce qu'on veut. Ainsi, le système de sauvegarde par l'interface Foris dont je parlais plus haut ne sauvegarde que `/etc/config`. Si on veut tout garder, on peut le faire avec un script et cron.

Pour faire quoi que ce soit sur l'Omnia, il vaut mieux connaitre OpenWrt (son Wiki <https://wiki.openwrt.org/>, ses forums <https://forum.openwrt.org/>...) Par exemple, si vous préférez joe à vi (et, non, je n'ai pas trouvé d'emacs sur OpenWrt, système conçu pour des engins contraints en ressources matérielles) :

```
root@turris:~# opkg list | grep -i editor
joe - 4.2-1 - Joe is world-famous Wordstar like text editor, that also features Emacs and Pico emulation
nano - 2.6.0-1 - Nano (Nano's ANOther editor, or Not ANOther editor) is an enhanced clone of the Pico text edito
vim - 7.4-3 - Vim is an almost compatible version of the UNIX editor Vi. (Tiny build)
zile - 2.3.24-4 - Zile is a small Emacs clone. Zile is a customizable, self-documenting real-time display editor
...

root@turris:~# opkg install joe
Installing joe (4.2-1) to root...
Downloading https://api.turris.cz/openwrt-repo/omnia/packages//packages/joe_4.2-1_mvebu.ipk.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  238k  100  238k    0     0   589k      0 --:--:-- --:--:-- --:--:--  602k
Configuring joe.
```

La configuration IPv6 ne s'est pas faite toute seule (ce n'est pas entièrement la faute du Turris mais un peu quand même). Par défaut, le Turris distribue sur le réseau local des ULA (RFC 4193) comme `fde8:9fa9:1aba:0:X:W:Y:Z`. Pour réaliser la configuration en étant connecté à Free, j'ai suivi un bon HOWTO de OpenWrt <`https://wiki.openwrt.org/doc/howto/freebox`> mais il y manque un point important, la route par défaut statique (à ce sujet, cela vaut aussi la peine de consulter la documentation OpenWrt sur le réseau <`https://wiki.openwrt.org/doc/uci/network`>). Donc, ce que j'ai du faire :

— Relever l'adresse locale au lien utilisée par l'Omnia sur la patte qui le connecte à la Freebox (`ifconfig eth1`),
— Sur la Freebox (`http://mafreebox.freebox.fr/`, « Paramètres de la Freebox » puis « Configuration IPv6 »), mettre cette adresse en "*Next hop*" pour le préfixe que nous a alloué Free,
— Au passage, notez sur la Freebox la valeur de ce préfixe alloué,
— Configurer le réseau de l'Omnia (`/etc/config/network`) comme indiqué dans le HOWTO ci-dessus,
— Ajouter une route statique sur l'Omnia (le HOWTO OpenWrt n'en parle pas).

Cela donc un `/etc/config/network` qui ressemble à (si `2001:db8:cafe:1234::1:fe/64` est le préfixe IPv6 alloué par Free, celui qu'on trouve dans l'interface Web de la Freebox) :

```
config interface 'lan'
option ifname 'eth0 eth2'
option force_link '1'
option type 'bridge'
option proto 'static'
option netmask '255.255.255.0'
option ipaddr '192.168.1.1'
option ip6addr '2001:db8:cafe:1234::1:fe/64'
option ip6prefix '2001:db8:cafe:1234::/64'
option ip6gw '2001:db8:cafe:1234::1'
option ip6assign '64'
option mtu '1452'

config interface 'wan'
option ifname 'eth1'
option proto 'dhcp'
        option mtu '1452'

config interface 'wan6'
option ifname '@wan'
option _orig_bridge 'false'
option proto 'static'
option ip6addr '2001:db8:cafe:1234::2/126'
option ip6gw '2001:db8:cafe:1234::1'
option ip6prefix '2001:db8:cafe:1234::/64'

# Route par défaut statique
config route6
option interface 'wan6'
option target '::/0'
option gateway 'fe80::f6ca:e5ff:fe4d:1f41'
```

Si vous êtes attentifs, vous aurez remarqué qu'on force une MTU à 1 452 octets. L'IPv6 de Free en ADSL n'étant pas natif (mais un tunnel 6rd, cf. RFC 5969), ce réglage était nécessaire pour éviter les symptômes habituels d'un problème de PMTUD (ping qui marche mais pas curl, etc).

Si votre FAI ne fournit pas IPv6, le Turris Omnia permet d'établir un tunnel, en théorie, mais je n'ai jamais testé.

Autre jouet amusant, le Turris a un pot de miel configurable, pour SSH et telnet. Les sessions capturées sont également transmises aux responsables du projet et visibles via le portail des utilisateurs (mon premier « pirate » venait de Turquie et a tapé `uname -a`).

Passons maintenant aux problèmes, car le logiciel a des bogues embêtantes. J'ai eu beaucoup d'ennuis avec le serveur NTP <https://discourse.labs.nic.cz/t/how-to-activate-the-ntp-server/1039>. Rien ne marchait. J'ai du finalement désactiver le serveur par défaut (/etc/config/system, option enabled '0') et ntpclient, puis installer ntpd qui, lui, fonctionne. (Normalement, sur OpenWrt, cela aurait du marcher tout seul <http://www.guiguishow.info/2011/08/24/installer-un-serveur>, la doc <https://wiki.openwrt.org/doc/howto/ntp.client> le dit). Attention, supprimer avec opkg le paquetage ntpclient ne suffit pas, la mise à jour automatique de l'Omnia le réinstalle <https://www.turris.cz/doc/en/howto/installation>. Maintenant, la synchronisation temporelle marche :

```
root@turris:~# ntpq
ntpq> peers
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+mx4.nic.fr      138.96.64.10     2 u  585 1024  377    8.661   -1.611   1.186
 webcgi1-g20.fre .INIT.          16 u    - 1024    0    0.000    0.000   0.000
 webcgi2-g20.fre .INIT.          16 u    - 1024    0    0.000    0.000   0.000
+pob01.aplu.fr   40.179.132.91    2 u  555 1024  377   10.465   -4.789   4.553
-host3.nuagelibr 138.96.64.10     2 u  193 1024  377   10.405    3.660   2.096
 vel.itat.io     131.188.3.223    2 u   98 1024    1   25.894    0.007   0.230
*cluster004.lino 82.95.215.61     2 u  557 1024  377    7.166   -0.876   0.973
```

Et les machines du réseau local peuvent se synchroniser sur le Turris. (Au passage, la commande ntpq est dans le paquetage ntp-utils.)

Second problème sérieux, avec le serveur SSH. Pour un certain nombre d'utilisateurs de l'Omnia <https://discourse.labs.nic.cz/t/ssh-server-configuration/915/>, la création des clés SSH de la machine se passe mal et des fichiers de taille zéro sont créés (et cela ne se produit pas uniquement, contrairement à ce que racontent certains, lors d'une coupure de courant). Cela empêche évidemment le serveur SSH de démarrer. On ne peut donc pas se connecter au shell pour arranger les choses. Il faut alors utiliser le port USB comme port série (je n'ai pas essayé) ou bien réparer le problème entièrement depuis LuCI ("*System*" puis "*Custom commands*") en exécutant de quoi rétablir le système. Et l'interface de LuCI est pénible pour cela (par exemple, ssh-keygen -N "" ne marchera pas car LuCI supprime la chaîne vide...). J'ai donc du définir des commandes rm -f /etc/ssh/ssh_host_ecdsa_key /etc/ssh/ssh_host_ecdsa_key.pub /etc/ssh/ssh_host_ecdsa_key /etc/ssh/ssh_host_ecdsa_key.pub /etc/ssh/ssh_host_rsa_key /etc/ssh/ssh_host_rsa_key.pub /etc/ssh/ssh_host_dsa_key /etc/ssh/ssh_host_dsa_key.pub /etc/ssh/ssh_host_ed25519_key /etc/ssh/ssh_host_ed25519_key.pub (eh non, pas droit aux jokers) puis ssh-keygen -A puis /etc/init.d/sshd start.

Autre méthode pour s'amuser, jouer avec les VLAN. En faisant une erreur dans la configuration du commutateur de l'Omnia, j'avais déclenché une tempête de trafic interne qui rendait le routeur totalement inutilisable. Même pas moyen de se connecter en SSH pour réparer. L'erreur étant dans la configuration, redémarrer ne servait à rien (l'Omnia n'a apparemment pas de mémorisation temporaire des configurations réseau potentiellement dangereuses, comme ça existe sur JunOS). Le port série aurait peut-être été une solution mais il y avait plus simple : remettre l'Omnia à sa configuration d'usine <https://www.turris.cz/doc/en/howto/omnia_factory_reset>, se reconnecter, et restaurer la configuration sauvegardée.

Voilà, prochaine étape, installer un serveur SNMP...

Quelques autres lectures sur le Turris Omnia :

— L'expérience de Juraj <http://juraj.bednar.sk/blog/2016/10/30/turris-omnia-review/> (il est sévère mais les problèmes qu'il note existent réellement).
— Mon deuxième article sur le Turris <https://www.bortzmeyer.org/turris-bis.html>, avec d'autres aventures.

PS : si vous voulez acheter un Turris Omnia (j'ai eu le mien via le "*crowdfunding*"), voyez cette annonce <https://www.nic.cz/page/3384/the-successful-open-source-router-turris-omnia-moves-f>.